Office of Information Technology Standard

# Security:  LDAP-enabled Directory Services

**Definition(s):**
LDAP-enabled directory services provide a means to share directory information with all agencies via standards-based LDAP clients and directory–enabled applications.

**Rationale:**
In order to fulfill the growing need for inter-agency access to information and to support web-based applications and portals,  the state must develop the means of centralizing employee records for application access authentication, e-mail address management, and access authorization to other LDAP server-based lists of information, and  provide for standards-based, centralized management of employee records.

In addition, the directory service must:
- scale
- be programmable
- support directory-enabled provisioning
- integrate seamlessly with the other stated standards, including the network operating system, workstation operating system, and applications.

**Approved Standards:**
- X.500 standards for global directory construction and replication across multiple servers.
- LDAP version 3 compliant access services, the preferred standard for read/write access to directories.
- Kerberos version 5 and X.509 for authentication.

**Approved Products:**
Microsoft Active Directory

**Guidelines/Technical Considerations:**
Directory services must be addressed in two areas:
 - the agency platform directory, which should be fully integrated into the statewide standard network operating system.
 - enterprise network, used for authentication, personalization, and access control between agencies via the intranet/extranet.

**Review Cycle:**
As needed

**Timeline:**
Issued:  September, 2002

**Transition:**
The Department of Public Safety is responsible for ownership of a root directory, and establishment of standards and guidelines for agency directory services that can be extended to the enterprise level.

**Procurement:**
Not applicable.

Date:  _____

Approved by:  _____